

WHAT IS CLAIMED IS:

1. A method of generating a pseudo-random bit series based on a given polynomial of order N, for M parallel communication lines using a system comprising: N flip-flop machines and logic circuit, said method comprising the steps of:
 - A. Initializing a series of N bits according to given initial values;
 - B. Storing current series of N bits in flip-flop machines;
 - C. Calculating a series of the next M bits using the N flip flop machines as function of the current N bit series wherein the function is based on first pre-generated equation;
 - D. Calculating the values of the next N bit using the N flip flop machines as function of the current N bit series wherein the function is based on a second pre-generated equation;
 - E. Repeating steps B till D for any new coming M bits;
2. The method of claim 1 wherein the generation of first and second equations is based the given polynomial expression;
3. The method of claim 2 wherein the generation of first and second equations comprise the steps of:

Optixnetworks

- 10 -

- A. Initializing a sequential set of first N rows in matrix array having N columns and M rows according to values of a unit diagonal matrix array having N rows and columns (wherein each row contain single digit of value 1 placed at the respective place according the serial order of the row);
 - B. Selecting at least two rows from previous N rows according to sequential order based on power values of the polynomial expression;
 - C. Calculating next row of N bits by conducting logic operation on selected rows;
 - D. Repeating steps B and C, M times until calculating the total of M+N rows;
 - E. Generating first equation as manipulation of the first M rows;
 - F. Generating second equation as manipulation of the rows: M+1, M+2 till M+N.
4. The method of claim 3 wherein the logic operation in step C is XOR.
 5. The method of claim 1 further comprising the steps of:
 - A. Compare the values of M and N according to equation:

$$M < 2^{N+1} / N;$$

- B. Perform steps A... D of claim 1 in case $M < (2^{N+1} / N)$;
- C. Perform the following steps in case $M > (2^{N+1} / N)$;
- D. Initializing a series of N bits according to shortest repeating sequence of a given pseudorandom series;
- E. Storing current series of N bits in flip-flop machines;
- F. Calculating a series of the next M bits as function of the current N bit series;
- G. Repeating steps E AND F for any new coming M bits;
6. A machine for generating a pseudo-random bit series base on a given polynomial of order N, for M parallel communication lines, said machine comprising:
- A. N flip-flop machines, storing current series of N bits Initialized by first series of N bits according to given initial values;
- B. A Logic circuit based on two pre-generated equations ("First equation" and "Second equation"), designated for calculating the next series of M and M+N bits using the N flip flop machines;
7. The method of claim 6 wherein the generation of first and second equations is based on known polynomial expression;

Optixnetworks

- 12 -

00004277-071204

8. The machine of claim 7 wherein the equations are generated by logic machine comprising:
- A. First logic component for generating transformation matrix of $M \times N$ order wherein each row is generated by recursive calculation as function previous N rows based on the known polynomial expression;
 - B. Second logic component for generating the first equation as manipulation of the first M rows;
 - C. Thirds logic component for generating second equation as manipulation of the rows: $M+1$, $M+2$ till $M+N$.
9. The machine of claim 8 wherein the logic circuit comprises XOR logic gates.

Optixnetworks

- 13 -